JP 01/772

02.02.01

EU

#4

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

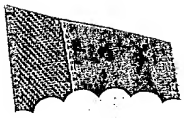
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　７月１１日

出願番号
Application Number: 特願２０００－２０９６７４

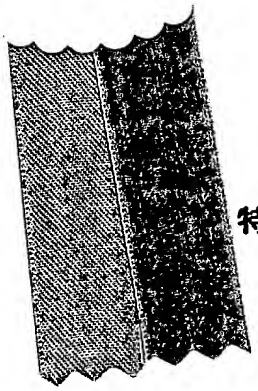
出願人
Applicant (s): ソニー株式会社

09193797



PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)



２００１年　３月　２日

特許庁長官
Commissioner,
Patent Office

及川耕造

出証番号　出証特２００１－３０１５１６１

【書類名】　特許願
【整理番号】　0000199003
【提出日】　平成12年 7月11日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/60
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　佐竹　清
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　金巻　裕史
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
　【代表者】　出井　伸之
【代理人】
　【識別番号】　100094053
　【弁理士】
　【氏名又は名称】　佐藤　隆久
【手数料の表示】
　【予納台帳番号】　014890
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9707389

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　認証装置、認証システムおよびその方法

【特許請求の範囲】

【請求項１】

第１の取り引き者に関する情報を保持し、第２の取り引き者に関する情報を保持する他の認証装置との間で通信を行いながらネットワークを介して行われる前記第１の取り引き者と前記第２の取り引き者との間の取り引きに関する認証を行う認証装置であって、

前記取り引き内容を示す情報と前記第２の取り引き者を特定する情報とを含む前記第１の取り引き者からの第１の要求に応じて、前記第２の取り引き者を特定する情報を含む第２の要求を前記第２の認証装置に送信し、前記第２の要求に応じた前記第２の認証装置による認証結果を示す第１の署名情報を受信し、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を前記第２の取り引き者が使用する装置に送信し、当該第３の要求に応じて前記第２の取り引き者が使用する装置から所定の応答を受ける送受信手段と、

前記所定の応答を受けた場合に、前記取り引きの履歴を記憶する記憶手段と、

前記所定の応答を受けた場合に、前記送受信手段を介して前記第１の取り引き者が使用する装置に送信される第２の署名情報であって、前記取り引きの正当性の認証結果を示す第２の署名情報を作成する署名作成手段と

を有する認証装置。

【請求項２】

暗号化手段

をさらに有し、

前記送受信手段は、前記第２の取り引き者との間の通信に用いる暗号鍵を前記第２の要求に応じて前記他の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第１の署名情報とを、前記第２の取り引き者が使用する装置に送信する

請求項１に記載の認証装置。

【請求項３】

前記送受信手段は、

前記他の認証装置が前記第２の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第２の取り引き者が使用する装置から受け、

前記記憶手段は、前記識別情報を用いて生成された前記取り引きの履歴を記憶する

請求項１に記載の認証装置。

【請求項４】

前記送受信手段は、前記第１の要求に含まれる前記取り引き内容に関する情報のうち、前記第１の取り引き者の課金に係わる情報以外の情報と、前記第１の署名情報とを含む第３の要求を前記第２の取り引き者が使用する装置に送信する

請求項１に記載の認証装置。

【請求項５】

前記送受信手段は、前記第１の要求に含まれる前記取り引き内容に関する情報と、前記第１の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第３の要求を前記第２の取り引き者が使用する装置に送信する

請求項１に記載の認証装置。

【請求項６】

前記取り引きに関する認証に対しての課金処理を行う課金処理手段

をさらに有する請求項１に記載の認証装置。

【請求項７】

前記課金処理手段は、前記他の認証装置との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う

請求項６に記載の認証装置。

【請求項８】

前記送受信手段は、前記第２の取り引き者が前記第１の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第２の取り引き者が使用する装置から、前記記所定の応答を受ける

請求項１に記載の認証装置。

【請求項９】

前記送受信手段は、

前記第２の署名情報を前記第２の取り引き者が使用する装置に送信する

請求項１に記載の認証装置。

【請求項１０】

ネットワークを介して少なくとも２者間で行われた取り引きを認証する認証方法システムにおいて、

第１の取り引き者に関する取り引きを認証する第１の認証装置と、

第２の取り引き者に関する取り引きを認証する第２の認証装置と

を有し、

前記第１の認証装置は、

前記取り引き内容を示す情報と前記第２の取り引き者を特定する情報とを含む前記第１の取り引き者による第１の要求に応じて、前記第２の取り引き者を特定する情報を含む第２の要求を前記第２の認証装置に送信し、前記第２の要求に応じた前記第２の認証装置による認証結果である第１の署名情報を受信し、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を前記第２の取り引き者が使用する装置に送信し、当該第３の要求に応じて前記第２の取り引き者から所定の応答を受けると、前記取り引きの履歴を記憶し、前記取り引きの正当性の認証結果を示す第２の署名情報を前記第１の取り引き者に提供する

認証システム。

【請求項１１】

前記第１の認証装置は、

暗号化手段

をさらに有し、

前記送受信手段は、前記第２の取り引き者との間の通信に用いる暗号鍵を前記第２の要求に応じて前記第２の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第１の署名情報とを、前記第２の取り引き者が使用する装置に送信する

請求項１０に記載の認証システム。

【請求項１２】

前記第１の認証装置の前記送受信手段は、

前記第２の認証装置が前記第２の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第２の取り引き者が使用する装置から受け、

前記記憶手段は、前記識別情報を用いて生成された前記取り引きの履歴を記憶する

請求項１０に記載の認証システム。

【請求項１３】

前記第１の認証装置は、

前記第２の署名情報を前記第２の取り引き者に提供する

請求項１０に記載の認証システム。

【請求項１４】

第１の取り引き者に関する取り引きを認証する第１の認証装置と、第２の取り引き者に関する取り引きを認証する第２の認証装置とを用いて、ネットワークを介して行われる前記第１の取り引き者と前記第２の取り引き者との間の取り引きに関する認証を行う認証方法であって、

前記第１の取り引き者から前記第１の認証装置に、前記取り引き内容を示す情報と前記第２の取り引き者を特定する情報とを含む第１の要求を出し、

前記第１の要求に応じて、前記第１の認証装置から前記第２の認証装置に、前記第２の取り引き者を特定する情報を含む第２の要求を送信し、

前記第２の要求に応じて、前記第２の認証装置からの前記第１の認証装置に、当該第２の認証装置による認証結果を示す第１の署名情報を送信し、

前記第１の認証装置から前記第２の取り引き者が使用する装置に、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を送信し、

当該第３の要求に応じて、前記第２の取り引き者が使用する装置から前記第１の認証装置に所定の応答を出し、

前記所定の応答に応じて、前記第１の認証装置は、前記取り引きの履歴を記憶

し、前記取り引きの正当性の認証結果を示す第２の署名情報を作成し、当該第２の署名情報を、前記第１の取り引き者が使用する装置に送信する

認証方法。

【請求項１５】

前記第２の取り引き者との間の通信に用いる暗号鍵を前記第２の要求に応じて、前記第２の認証装置から前記第１の認証装置に送信し、

前記第１の認証装置は、前記取り引き内容に関する情報と前記第１の署名情報とを、前記暗号鍵を用いて暗号化した後に、前記第２の取り引き者が使用する装置に送信する

請求項１４に記載の認証方法。

【請求項１６】

前記第１の認証装置は、前記第２の認証装置が前記第２の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第２の取り引き者が使用する装置から受け、前記識別情報を用いて生成された前記取り引きの履歴を記憶する

請求項１４に記載の認証方法。

【請求項１７】

前記第１の要求に含まれる前記取り引き内容に関する情報のうち、前記第１の取り引き者の課金に係わる情報以外の情報と、前記第１の署名情報とを含む第３の要求を、前記第１の認証装置から前記第２の取り引き者が使用する装置に送信する

請求項１４に記載の認証方法。

【請求項１８】

前記第１の要求に含まれる前記取り引き内容に関する情報と、前記第１の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第３の要求を、前記第１の認証装置から前記第２の取り引き者が使用する装置に送信する

請求項１４に記載の認証方法。

【請求項１９】

前記第１の認証装置と前記第２の認証装置との間で、前記取り引きに関する認

証に対して行う課金の割合を決定するための処理を行う

請求項１４に記載の認証方法。

【請求項２０】

前記第２の取り引き者が前記第１の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第２の取り引き者が使用する装置から前記第１の認証装置に、前記所定の応答を出す

請求項１４に記載の認証方法。

【請求項２１】

前記第１の認証装置から前記第２の取り引き者が使用する装置に、前記第２の署名情報を送信する

請求項１４に記載の認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子商取引情報を認証する認証装置、認証システムおよびその方法に関する。

【０００２】

【従来の技術】

インターネットなどのネットワークを介して商品等の販売や代金の決済を行う電子商取引が普及している。

このような電子商取引を用いて利用者が商品等を購入する場合には、例えば、利用者が店舗や各家庭に設置されたパーソナルコンピュータなどの発注者端末装置を操作して、ネットワークを介して、商品等の販売を行うサーバ装置にアクセスを行う。これにより、サーバ装置から発注者端末装置に商品の写真、特性および価格などの情報が提供され、発注者端末装置のディスプレイに表示される。利用者は、このような情報を見ながら、購入を希望する商品等を選択し、選択した商品等の発注処理を行う。発注処理は、利用者個人を認証する個人認証情報、購入を希望する商品等を指定した情報およびその決済方法等の情報を、発注者端末装置を操作して入力し、これをネットワークを介してサーバ装置に送信する。

【０００３】

このような電子商取引では、ネットワーク銀行などが、ネットワークを介した取り引きに関しての決済業務を行うが、当該決済を行うに当たって、決済対象となる電子商取引の内容の正当性が認証されている必要がある。

従って、電子商取引では、このような電子商取引の内容の正当性を認証する認証装置が用いられる。当該認証装置を用いた認証業務は、ネットワーク銀行、あるいは他の信頼性のある機関が行う。

【０００４】

【発明が解決しようとする課題】

ところで、上述したような電子商取引が普及すると、複数に認証機関が、電子商取引の認証業務を行うことになる。

この場合に、同じ電子商取引に参加した利用者が、それぞれ異なる認証機関と契約をしている場合に、どのようにして当該電子商取引の正当性を認証するかが課題となる。

この場合に、同じ電子商取引に参加した利用者が契約した複数の認証機関で、、利用者の情報を共有することで、上述した課題に対処できるが、利用者の個人情報が、他の機関に漏れてしまうという問題がある。

【０００５】

本発明は上述した従来技術の問題点に鑑みてなされ、異なる認証機関と契約した利用者相互間の取り引きの認証を、利用者の個人情報を他の認証機関に提供することなく、高い信頼性で行うことができる認証装置、認証システムおよびその方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第１の発明の認証装置は、第１の取り引き者に関する情報を保持し、第２の取り引き者に関する情報を保持する他の認証装置との間で通信を行いながらネットワークを介して行われる前記第１の取り引き者と前記第２の取り引き者との間の取り引きに関する認証を行う認証装置であって、前記取り引き内容を示す情報と前記第２

の取り引き者を特定する情報とを含む前記第１の取り引き者からの第１の要求に応じて、前記第２の取り引き者を特定する情報を含む第２の要求を前記第２の認証装置に送信し、前記第２の要求に応じた前記第２の認証装置による認証結果を示す第１の署名情報を受信し、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を前記第２の取り引き者が使用する装置に送信し、当該第３の要求に応じて前記第２の取り引き者が使用する装置から所定の応答を受ける送受信手段と、前記所定の応答を受けた場合に、前記取り引きの履歴を記憶する記憶手段と、前記所定の応答を受けた場合に、前記送受信手段を介して前記第１の取り引き者が使用する装置に送信される第２の署名情報であって、前記取り引きの正当性の認証結果を示す第２の署名情報を作成する署名作成手段とを有する。

【０００７】

第１の発明の認証装置の作用は以下のようになる。

送受信手段、前記取り引き内容を示す情報と前記第２の取り引き者を特定する情報とを含む前記第１の取り引き者からの第１の要求を受ける。

そして、当該第２の要求に応じて、前記第２の取り引き者を特定する情報を含む第２の要求が、前記送受信手段から前記第２の認証装置に送信される。

次に、送受信手段は、前記第２の要求に応じた第１の署名情報を前記第２の認証装置から受信する。

次に、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を、前記送受信手段から前記第２の取り引き者が使用する装置に送信する。

次に、送受信手段は、当該第３の要求に応じて前記第２の取り引き者が使用する装置から所定の応答を受ける。

前記送受信手段が前記所定の応答を受けると、記憶手段に、前記取り引きの履歴が記憶される。

また、前記送受信手段が前記所定の応答を受けると、署名作成手段によって、前記取り引きの正当性を認証する第２の署名情報が作成され、当該第２の署名情報が、前記送受信手段を介して前記第１の取り引き者が使用する装置に送信され

る。

【０００８】

また、第１の発明の認証装置は、好ましくは、暗号化手段をさらに有し、前記送受信手段は、前記第２の取り引き者との間の通信に用いる暗号鍵を前記第２の要求に応じて前記他の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第１の署名情報とを、前記第２の取り引き者が使用する装置に送信する。

【０００９】

また、第１の発明の認証装置は、好ましくは、前記送受信手段は、前記他の認証装置が前記第２の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第２の取り引き者が使用する装置から受け、前記記憶手段は、前記識別情報を用いて生成された前記取り引きの履歴を記憶する。

【００１０】

また、第１の発明の認証装置は、好ましくは、前記送受信手段は、前記第１の要求に含まれる前記取り引き内容に関する情報のうち、前記第１の取り引き者の課金に係わる情報以外の情報と、前記第１の署名情報とを含む第３の要求を前記第２の取り引き者が使用する装置に送信する。

【００１１】

また、第１の発明の認証装置は、好ましくは、前記送受信手段は、前記第１の要求に含まれる前記取り引き内容に関する情報と、前記第１の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第３の要求を前記第２の取り引き者が使用する装置に送信する。

【００１２】

また、第１の発明の認証装置は、好ましくは、前記取り引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する。

【００１３】

また、第１の発明の認証装置は、好ましくは、前記課金処理手段は、前記他の認証装置との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う。

【００１４】

また、第１の発明の認証装置は、好ましくは、前記送受信手段は、前記第２の取り引き者が前記第１の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第２の取り引き者が使用する装置から、前記記所定の応答を受ける。

【００１５】

また、第２の発明の認証システムは、ネットワークを介して少なくとも２者間で行われた取り引きを認証する認証方法システムであって、第１の取り引き者に関する取り引きを認証する第１の認証装置と、第２の取り引き者に関する取り引きを認証する第２の認証装置とを有し、前記第１の認証装置は、前記取り引き内容を示す情報と前記第２の取り引き者を特定する情報とを含む前記第１の取り引き者による第１の要求に応じて、前記第２の取り引き者を特定する情報を含む第２の要求を前記第２の認証装置に送信し、前記第２の要求に応じた前記第２の認証装置からの第１の署名情報を受信し、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を前記第２の取り引き者が使用する装置に送信し、当該第３の要求に応じて前記第２の取り引き者から所定の応答を受けると、前記取り引きの履歴を記憶し、前記取り引きの正当性を認証する第２の署名情報を前記第１の取り引き者に提供する。

【００１６】

また、第２の発明の認証システムは、前記第１の認証装置は、暗号化手段をさらに有し、前記送受信手段は、前記第２の取り引き者との間の通信に用いる暗号鍵を前記第２の要求に応じて前記第２の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第１の署名情報とを、前記第２の取り引き者が使用する装置に送信する。

【００１７】

また、第３の発明の認証方法は、第１の取り引き者に関する取り引きを認証する第１の認証装置と、第２の取り引き者に関する取り引きを認証する第２の認証装置とを用いて、ネットワークを介して行われる前記第１の取り引き者と前記第２の取り引き者との間の取り引きに関する認証を行う認証方法であって、前記第

１の取り引き者から前記第１の認証装置に、前記取り引き内容を示す情報と前記第２の取り引き者を特定する情報とを含む第１の要求を出し、前記第１の要求に応じて、前記第１の認証装置から前記第２の認証装置に、前記第２の取り引き者を特定する情報を含む第２の要求を送信し、前記第２の要求に応じて、前記第２の認証装置からの前記第１の認証装置に、当該第２の認証装置による認証結果を示す第１の署名情報を送信し、前記第１の認証装置から前記第２の取り引き者が使用する装置に、前記第１の要求に含まれる前記取り引き内容に関する情報と前記第１の署名情報とを含む第３の要求を送信し、当該第３の要求に応じて、前記第２の取り引き者が使用する装置から前記第１の認証装置に所定の応答を出し、前記所定の応答に応じて、前記第１の認証装置は、前記取り引きの履歴を記憶し、前記取り引きの正当性の認証結果を示す第２の署名情報を作成し、当該第２の署名情報を、前記第１の取り引き者が使用する装置に送信する。

【００１８】

また、第３の発明の認証方法は、好ましくは、前記第２の取り引き者との間の通信に用いる暗号鍵を前記第２の要求に応じて、前記第２の認証装置から前記第１の認証装置に送信し、前記第１の認証装置は、前記取り引き内容に関する情報と前記第１の署名情報とを、前記暗号鍵を用いて暗号化した後に、前記第２の取り引き者が使用する装置に送信する。

【００１９】

【発明の実施の形態】

以下、本発明の実施形態に係わるトランザクション認証システムについて説明する。

図１は、本実施形態のトランザクション認証システム１の全体構成図である。

図１に示すように、トランザクション認証システム１では、例えば、発注者３１の発注者端末装置１１と、受注者３３の受注者端末装置１５と、ネットワーク銀行４０の認証装置５０と、ネットワーク銀行４１の認証装置５１とが、インターネットなどのネットワーク（通信網）を介して接続されており、発注者３１と受注者３３との間のトランザクション（取り引き）の正当性を認証する。

【００２０】

本実施形態では、例えば、発注者３１とネットワーク銀行４０との間で認証を行うことに関しての契約が成されており、受注者３３とネットワーク銀行４１との間で認証を行うことに関しての契約が成されている。

また、ネットワーク銀行４０とネットワーク銀行４１とでは、認証に関して、相互に連携する旨の相互乗り入れの契約が成されている。

【００２１】

本実施形態では、発注者３１が本発明の第１の取り引き者に対応し、受注者３３が本発明の第２の取り引き者に対応している。

また、認証装置５０が、第１の発明の認証装置、並びに第２の発明および第３の発明の第１の認証装置に対応している。

また、認証装置５１が、第１の発明の他の認証装置、並びに第２の発明および第３の発明の第２の認証装置に対応している。

【００２２】

以下、トランザクション認証システム１を構成する各装置について説明する。

〔発注者端末装置１１〕

図２に示すように、発注者端末装置１１は、例えば、発注者３１の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部６１、送信部６２、暗号化部６３、復号部６４、記憶部６５、制御部６６および署名検証部６７を有する。

なお、発注者端末装置１１は、例えば、発注者３１が使用する際に、発注者３１の指紋等の身体的特徴から得られる情報と、予め記憶部６５に予め記憶してある身体的特徴を示す情報とを比較することで、発注者３１が正当な使用者であることを認証する生態認証部を有していてもよい。

【００２３】

受信部６１は、ネットワークを介して認証装置５０から情報あるいは要求を受信する。

送信部６２は、ネットワークを介して認証装置５０に情報あるいは要求を送信する。

また、受信部６１および送信部６２は、受注者３３が提供する商品等の案内情

報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部６３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部６４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部６５は、例えば、発注者３１がネットワーク銀行４０と契約を行うと、例えば、発注者３１に割り当てられた秘密鍵$K_{31,S}$などを格納する。

制御部６６は、発注者端末装置１１内の各構成要素の処理を統括的に制御する。

署名検証部６７は、例えば、認証装置５０が作成した署名情報を、ネットワーク銀行４０の公開鍵$K_{40,P}$を用いて検証する。

【００２４】

〔受注者端末装置１５〕

図３に示すように、受注者端末装置１５は、サイバーモール(Cyber Moll)などに店舗を出している受注者３３が使用するサーバ装置であり、受信部７１、送信部７２、暗号化部７３、復号部７４、記憶部７５、制御部７６および署名検証部７７を有する。

受信部７１は、ネットワークを介して認証装置５０，５１から情報あるいは要求を受信する。

送信部７２は、ネットワークを介して認証装置５０，５１に情報あるいは要求を送信する。

また、受信部７１および送信部７２は、発注者端末装置１１からのアクセスに応じて、例えば、記憶部７５から読み出した受注者３３が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置１１に送信する。

暗号化部７３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部７４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部７５は、例えば、受注者３３がネットワーク銀行４１と契約を行うと、例えば、受注者３３に割り当てられた秘密鍵$K_{33,S}$などを格納する。

制御部７６は、受注者端末装置１５内の各構成要素の処理を統括的に制御する。

署名検証部７７は、例えば、受注者３３の公開鍵$K_{33,P}$を用いて、受注者端末装置１５が作成した署名情報の検証を行う。

【００２５】

〔認証装置５０〕

図４に示すように、認証装置５０は、受信部８１、送信部８２、暗号化部８３、復号部８４、記憶部８５、制御部８６、署名作成部８７および課金処理部８８を有する。

ここで、受信部８１および送信部８２が、第１の発明の送受信手段に対応し、記憶部８５が第１の発明の記憶手段に対応し、署名作成部８７が第１の発明の署名作成手段に対応している。

【００２６】

受信部８１は、ネットワークを介して発注者端末装置１１、受注者端末装置１５および認証装置５１から情報あるいは要求を受信する。

送信部８２は、ネットワークを介して発注者端末装置１１、受注者端末装置１５および認証装置５１に情報あるいは要求を送信する。

暗号化部８３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部８４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部８５は、例えば、発注者３１がネットワーク銀行４０と契約を行うと、例えば、発注者３１に割り当てられた秘密鍵$K_{31,S}$に対応する公開鍵$K_{33,P}$などを格納する。

制御部８６は、認証装置５０内の各構成要素の処理を統括的に制御する。

署名作成部８７は、ネットワーク銀行４０の秘密鍵$K_{40,S}$を用いて署名情報の作成を行う。

課金処理部８８は、発注者３１による取り引きに関する認証に対しての課金処理を行い、認証装置５１との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う。

認証装置５０の各構成要素の詳細な処理については、後述する動作例で記載する。

【００２７】

図５に示すように、認証装置５１は、受信部９１、送信部９２、暗号化部９３、復号部９４、記憶部９５、制御部９６、署名作成部９７および課金処理部９８を有する。

受信部９１は、ネットワークを介して受注者端末装置１５および認証装置５０から情報あるいは要求を受信する。

送信部９２は、ネットワークを介して受注者端末装置１５および認証装置５０に情報あるいは要求を送信する。

暗号化部９３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部９４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部９５は、受注者３３がネットワーク銀行４１と契約を行うと、例えば、受注者３３に割り当てられた秘密鍵$K_{33,S}$に対応する公開鍵$K_{33,P}$などを格納する。

制御部９６は、認証装置５１内の各構成要素の処理を統括的に制御する。

署名作成部９７は、ネットワーク銀行４１の秘密鍵$K_{41,S}$を用いて署名情報の作成を行う。

課金処理部９８は、受注者３３による取り引きに関する認証に対しての課金処理を行い、認証装置５０との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う。

【００２８】

以下、トランザクション認証システム１の動作例を説明する。

以下に示す動作例を開始する前提として、発注者３１とネットワーク銀行４０との間で所定の契約が結ばれ、ネットワーク銀行４０は、発注者３１に対して、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１を発行する。ネットワーク銀行４０は、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１の対応表を図４に示す認証装置５０の記憶部８５に記憶する。ここで、個人キー情報ｋ１は、例えば、ネットワーク銀行４０と契約した契約者（発注者３１）の契約番号などの個人情報を示す識別子である。また、個人ＩＤ情報ＩＤ１は、発注者３１の銀行口座番号などの課金に係わる情報を示す識別子である。

また、ネットワーク銀行４０は、自らの秘密鍵$K_{40,S}$を図４に示す認証装置５０の記憶部８５に記憶すると共に、当該秘密鍵$K_{40,S}$に対応する公開鍵$K_{40,P}$を発注者端末装置１１に送信する。発注者端末装置１１は、公開鍵$K_{40,P}$を図２に示す記憶部６５に記憶する。

【００２９】

また、受注者３３とネットワーク銀行４１との間で所定の契約が結ばれ、ネットワーク銀行４１は、受注者３３に対して、個人キー情報Ｚおよび個人ＩＤ情報ＩＤ２を発行する。ネットワーク銀行４１は、個人キー情報Ｚおよび個人ＩＤ情報ＩＤ２の対応表を図５に示す認証装置５１の記憶部９５に記憶する。

また、ネットワーク銀行４１は、自らの秘密鍵$K_{41,S}$を図５に示す認証装置５１の記憶部９５に記憶すると共に、当該秘密鍵$K_{41,S}$に対応する公開鍵$K_{41,P}$を受注者端末装置１５に送信する。受注者端末装置１５は、公開鍵$K_{41,P}$を図３に示す記憶部７５に記憶する。

【００３０】

また、ネットワーク銀行４０とネットワーク銀行４１との間では、認証に関して相互乗り入れの契約がなされている。なお、認証装置５０と認証装置５１との間では、当該契約に基づいて、要求および情報の伝送が、公開鍵暗号方式あるいは共通鍵暗号方式を用いて行われる。

【００３１】

図６は、トランザクション認証システム１の動作例を説明するための図である。

ステップＳＴ１：

発注者端末装置１１は、図１に示す発注者３１は、例えばネットワーク上の商店である受注者３３に商品を発注する場合に、受注者３３を特定する情報（例えば受注者３３の名前）、発注する商品名および数量などを示す発注情報ａ１と、発注者３１の個人キー情報ｋ１と、発注者３１の個人ＩＤ情報ＩＤ１とを、図示しない操作手段を操作して発注者端末装置１１に入力する。なお、発注情報ａ１には、受注者３３を特定する情報が含まれている。

次に、図２に示す発注者端末装置１１の暗号化部６３は、記憶部６５から読み

出した所定の暗号鍵を用いて、発注情報ａ１と、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１を暗号化し、当該暗号化した情報を格納した認証要求ｉｎｆ１（本発明の第１の要求）を、送信部６２からネットワークを介して、図１に示すネットワーク銀行４０に送信する。

【００３２】

ステップＳＴ２：

図４に示す認証装置５０は、発注者端末装置１１からの認証要求ｉｎｆ１を受信部８１が受信すると、記憶部８５から所定の暗号化鍵を読み出し、復号部８４において、当該暗号鍵を用いて認証要求ｉｎｆ１を復号する。

次に、認証装置５０は、制御部８６の制御に基づいて、上記復号した認証要求ｉｎｆ１に格納された発注情報ａ１に含まれる受注者３３を特定する情報ｂ１を格納した要求ｉｎｆ２（本発明の第２の要求）を、記憶部８５から読み出した所定の暗号鍵を用いて暗号化部８３で暗号化した後に、受信部８１からネットワークを介して認証装置５１に送信する。

【００３３】

ステップＳＴ３：

図５に示す認証装置５１の制御部９６は、認証装置５０からの要求ｉｎｆ２を受信部９１が受信すると、記憶部９５から読み出した所定の暗号鍵を用いて復号部９４において当該要求ｉｎｆ２を復号する。

次に、署名作成部９７は、当該復号された要求ｉｎｆ２に格納された受注者３３を特定する情報ｂ１に対応する受注者３３の公開鍵$K_{33,P}$を記憶部８５から読み出し、当該公開鍵$K_{33,P}$について、記憶部８５から読み出した自らの秘密鍵$K_{41,S}$を用いて自らの認証結果を示す署名情報Ａｕ－Ｂ（本発明の第１の署名情報）を作成する。

次に、暗号化部９３は、受注者３３の公開鍵$K_{33,P}$および署名情報Ａｕ－Ｂを格納した応答ｉｎｆ３を、記憶部９５から読み出した所定の暗号鍵を用いて暗号化した後に、送信部９２から、、ネットワークを介して認証装置５０に送信する。

【００３４】

ステップＳＴ４：

図４に示す認証装置５０の復号部８４は、認証装置５１からの応答ｉｎｆ３を受信部８１が受信すると、記憶部８５から読み出した所定の暗号鍵を用いて、応答ｉｎｆ３を復号する。

次に、署名作成部８７は、ステップＳＴ２で復号した要求ｉｎｆ１に格納された発注情報ａ１および個人キー情報ｋ１を格納した情報ｉｎｆ１’と、上記復号された応答ｉｎｆ３に格納された署名情報Ａｕ－Ｂと、記憶部８５から読み出した自らの公開鍵$K_{40,P}$とについて、記憶部８５から読み出した自らの秘密鍵$K_{40,S}$を用いて署名情報Ａｕ－Ａ１を作成する。

次に、制御部８６は、情報ｉｎｆ１’と、署名情報Ａｕ－Ｂと、自らの公開鍵$K_{40,P}$と、上記生成した署名情報Ａｕ－Ａ１とを格納した要求ｉｎｆ４（本発明の第３の要求）を生成する。

次に、暗号化部８３は、ステップＳＴ４で認証装置５１から受信した受注者３３の公開鍵$K_{33,P}$を用いて、上記生成した要求ｉｎｆ４を暗号化した後に、送信部８２から、ネットワークを介して受注者端末装置１５に送信する。

【００３５】

ステップＳＴ５：

受注者端末装置１５の復号部７４は、認証装置５０からの要求ｉｎｆ４を受信部７１が受信すると、記憶部７５から読み出した自らの秘密鍵$K_{33,S}$を用いて、要求ｉｎｆ４を復号する。

次に、受注者端末装置１５の署名検証部７７は、上記復号した要求ｉｎｆ４に格納された署名情報Ａｕ－Ｂを、記憶部７５から読み出した認証装置５１の公開鍵$K_{41,P}$を用いて検証する。また、署名情報検証部は、上記復号した要求ｉｎｆ４に格納された認証装置５０の公開鍵$K_{40,P}$を用いて、要求ｉｎｆ４に格納された署名情報Ａｕ－Ａ１を検証する。

【００３６】

受注者端末装置１５の制御部７６は、署名検証部が上記検証の結果、署名情報Ａｕ－Ｂ，Ａｕ－Ａ１の正当性が認証されると、要求ｉｎｆ４に格納された情報ｉｎｆ１’と、署名情報Ａｕ－Ｂ，Ａｕ－Ａ１と、自らの個人キー情報Ｚとを格

納した応答ｉｎｆ５（本発明の所定の応答）を生成する。

次に、受注者端末装置１５の送信部７２は、上記生成した応答ｉｎｆ５を、上記復号した要求ｉｎｆ４に格納された認証装置５０の公開鍵$K_{40,P}$を用いて復号した後に、送信部７２から、ネットワークを介して認証装置５０に送信する。

受注者端末装置１５によって、署名情報Ａｕ－Ｂ，Ａｕ－Ａ１の正当性が認証されると、受注者３３は、例えば、要求Ｉｎｆ４に格納された情報Ｉｎｆ１’内の発注情報ａ１に基づいて、発注者３１が発注した商品等を発注者３１に発送したり、発注者３１が注文したサービスを発注者３１に提供する。

【００３７】

ステップＳＴ６：

認証装置５０の復号部８４は、受注者端末装置１５からの応答ｉｎｆ５を受信部８１が受信すると、記憶部８５から読み出した自らの秘密鍵$K_{40,S}$を用いて、ｉｎｆ５を復号し、要求ｉｎｆ１に格納された発注情報ａ１と、当該復号されたｉｎｆ５に格納された受注者３３の個人キー情報Ｚとを用いて、所定の取り引き履歴情報を作成し、これを記憶部８５に格納する。当該履歴情報は、ネットワーク銀行４０が、発注者３１に対して決済を行う際に用いられる。

また、認証装置５０の署名作成部８７は、ステップＳＴ２で受信した要求ｉｎｆ１と、応答ｉｎｆ５に含まれる受注者３３の個人キー情報Ｚと、ステップＳＴ４で作成した署名情報Ａｕ－Ａ１とについて、自らの秘密鍵$K_{40,S}$を用いて自らの認証結果を示す署名情報Ａｕ－Ａ２（本発明の第２の署名情報）を作成する。

次に、認証装置５０の制御部８６は、要求ｉｎｆ１と、個人キー情報Ｚと、署名情報Ａｕ－Ａ１と、署名情報Ａｕ－Ａ２とを格納した応答ｉｎｆ６を作成する。

【００３８】

次に、認証装置５０の暗号化部８３は、上記作成した応答ｉｎｆ６を、認証装置５０から読み出した所定の暗号鍵を用いて暗号化した後に、送信部８２から、ネットワークを介して発注者端末装置１１に送信する。

発注者端末装置１１では、受信した応答ｉｎｆ６を、図２示す記憶部６５から読み出した所定の暗号鍵を用いて復号部６４で復号する。

次に、発注者端末装置１１の署名検証部６６は、当該復号した応答ｉｎｆ６に格納された署名情報Ａｕ－Ａ１，Ａｕ－Ａ２を、記憶部６５から読み出したネットワーク銀行４０の公開鍵$K_{40,P}$を用いて検証することで、受注者端末装置１５との間の当該取り引きが正当に認証されたことを確認する。

【００３９】

以上説明したように、トランザクション認証システム１によれば、認証装置５０から認証装置５１へは、発注者３１の個人キー情報ｋ１および個人ＩＤ情報ＩＤ１を送信しないことから、発注者３１の個人情報が、発注者３１が契約していない他のネットワーク銀行４１に漏れることを回避できる。

【００４０】

また、トランザクション認証システム１によれば、認証装置５０が、認証装置５１から受けた受注者３３の公開鍵$K_{33,P}$および署名情報Ａｕ－Ｂを用いて、受注者３３の受注者端末装置１５との間で直接通信を行うことで、当該取り引きの履歴を認証装置５０に格納できる。

また、トランザクション認証システム１によれば、受注者３３は、自らの契約した認証装置５０の署名情報Ａｕ－Ｂを検証することで、当該取り引きの正当性を確認できる。

また、トランザクション認証システム１によれば、認証装置５０と５１との間では、図６に示す要求ｉｎｆ２およびｉｎｆ３を伝送するだけで、発注者３１と受注者３３との間の取り引きを認証でき、認証装置５０と５１との間の通信量を小さくできる。

【００４１】

また、トランザクション認証システム１によれば、図４に示す認証装置５０の課金処理部８８と、図５に示す認証装置５１の課金処理部９８との間で通信を行うことで、発注者３１と受注者３３との間の取り引きに関する認証に対して行う課金の割合を柔軟に決定できる。

【００４２】

上述したように、トランザクション認証システム１によれば、異なる認証機関と契約をしている複数の取り引き者の間の取り引きに関する認証を、高い信頼性

で、しかも効率的に行うことができる。その結果、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などを費用を低額にでき、電子商取引をさらに普及させることが可能になる。

【００４３】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、ネットワーク銀行４０，４１が、それぞれ認証装置５０，５１を用いて、トランザクション（取り引き）の認証業務を行う場合を例示したが、ネットワーク銀行４０，４１とは別の機関が、認証装置５０，５１を用いてトランザクションの認証業務を行うようにしてもよい。

【００４４】

また、上述した実施形態では、発注者３１が契約したネットワーク銀行４０の認証装置５０と、受注者３３が契約したネットワーク銀行４１の認証装置５１との間で連携して認証処理を行う場合を例示したが、３人以上の取り引き者がそれぞれ異なる認証機関と契約を行っている場合に、３以上の認証装置間で連携して認証処理を行う場合にも、本発明は適用可能である。

【００４５】

また、上述した実施形態では、図６に示すステップＳＴ１のように、暗号化された発注情報ａ１と、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１とを含む認証要求Ｉｎｆ１を、発注者端末装置１１から認証装置５０に送信する場合を例示したが、発注情報ａ１および個人キー情報ｋ１を含む認証要求Ｉｎｆ１を、発注者端末装置１１から認証装置５０に送信してもよい。このようにすれば、課金に係わる情報である個人ＩＤ情報ＩＤ１はネットワークを介して伝送されないため、ネットワーク上で個人ＩＤ情報ＩＤ１が不正に取得され、悪用されることを回避できる。

【００４６】

また、本発明では、例えば、認証装置５０から受注者端末装置１５に、署名情報Ａｕ－Ａ２（本発明の第２の署名情報）を送信するようにしてもよい。

【００４７】

【発明の効果】

以上説明したように、本発明によれば、例えば異なる認証機関と契約した複数の取り引き者間での取り引きの認証を、取り引き者の個人情報を他の認証機関に提供することなく、高い信頼性で行うことができる認証装置、認証システムおよびその方法を提供できる。

【図面の簡単な説明】

【図１】

図１は、本発明の実施形態のトランザクション認証システムの全体構成図である。

【図２】

図２は、図１に示す発注者端末装置の構成図である。

【図３】

図３は、図１に示す受注者端末装置の構成図である。

【図４】

図４は、図１に示す認証装置（Ａ）の構成図である。

【図５】

図５は、図１に示す認証装置（Ｂ）の構成図である。

【図６】

図６は、図１に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

【符号の説明】

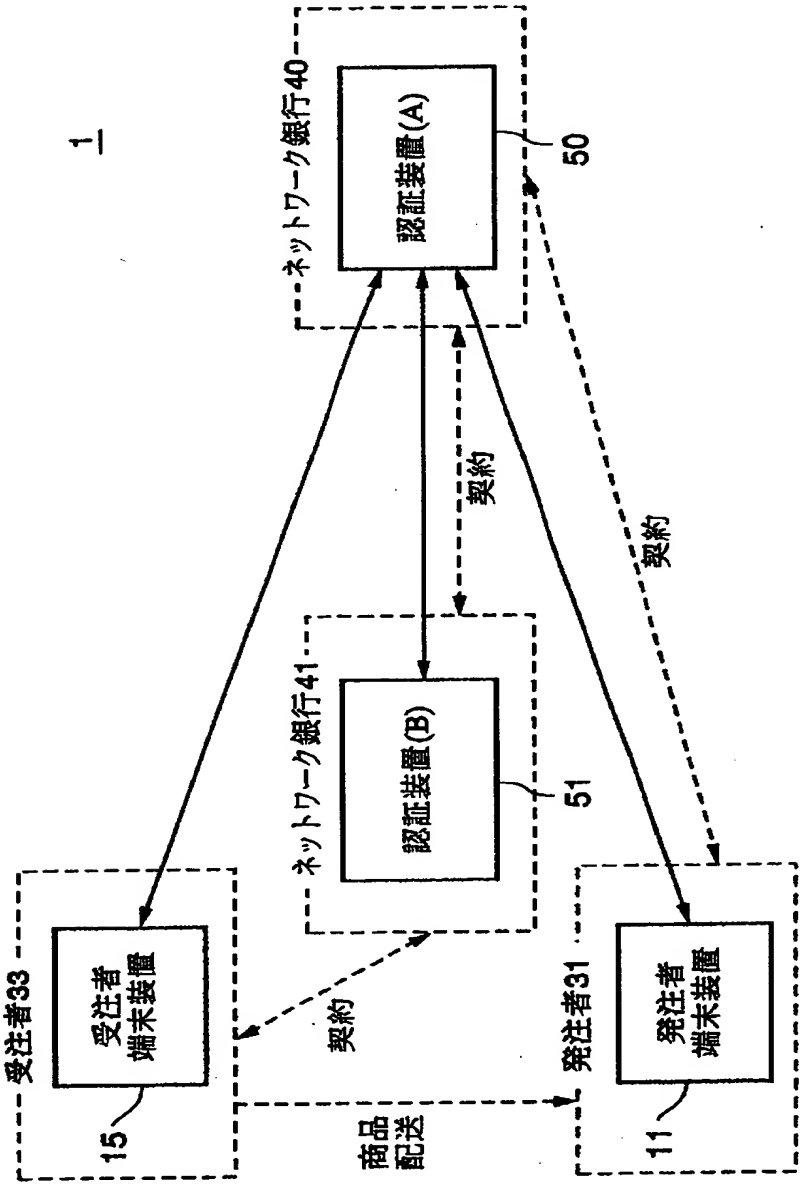
１…トランザクション認証システム、１１…発注者端末装置、１５…受注者端末装置、３１…発注者、３３…受注者、４０，４１…ネットワーク銀行、５０，５１…認証装置、６１，７１，８１，９１…受信部、６２，７２，８２，９２…送信部、６３，７３，８３，９３…暗号化部、６４，７４，８４，９４…復号部、６５，７５，８５，９５…記憶部、６６，７６，８６，９６…制御部、６７，７７…署名検証部、，８７，９７…署名作成部、８８，９８…課金処理部

ａ１…発注情報、ｋ１…発注者３１の個人キー情報ｋ１、ＩＤ１…発注者３１の個人ＩＤ情報、ｂ１…受注者を特定する情報、Ａｕ－Ｂ…認証装置５１の署名情報、Ａｕ－Ａ１，Ａｕ－Ａ２…認証装置５０のい署名情報、Ｚ…受注者の個人

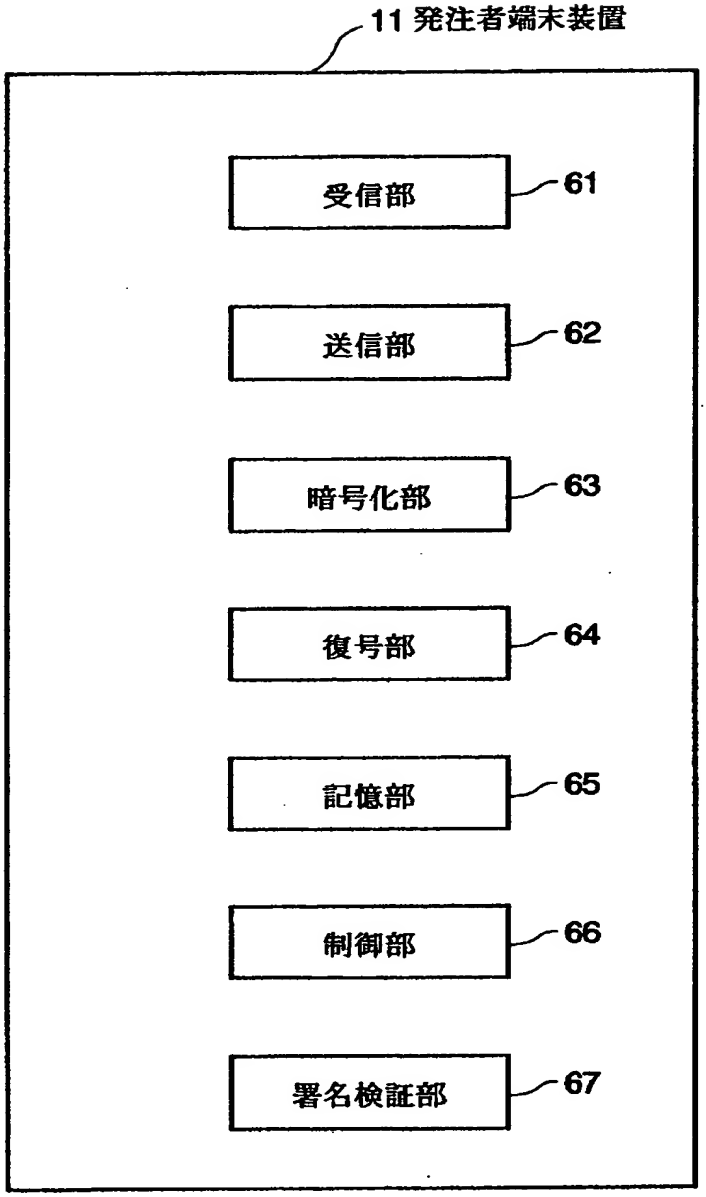
キー情報

【書類名】　図面

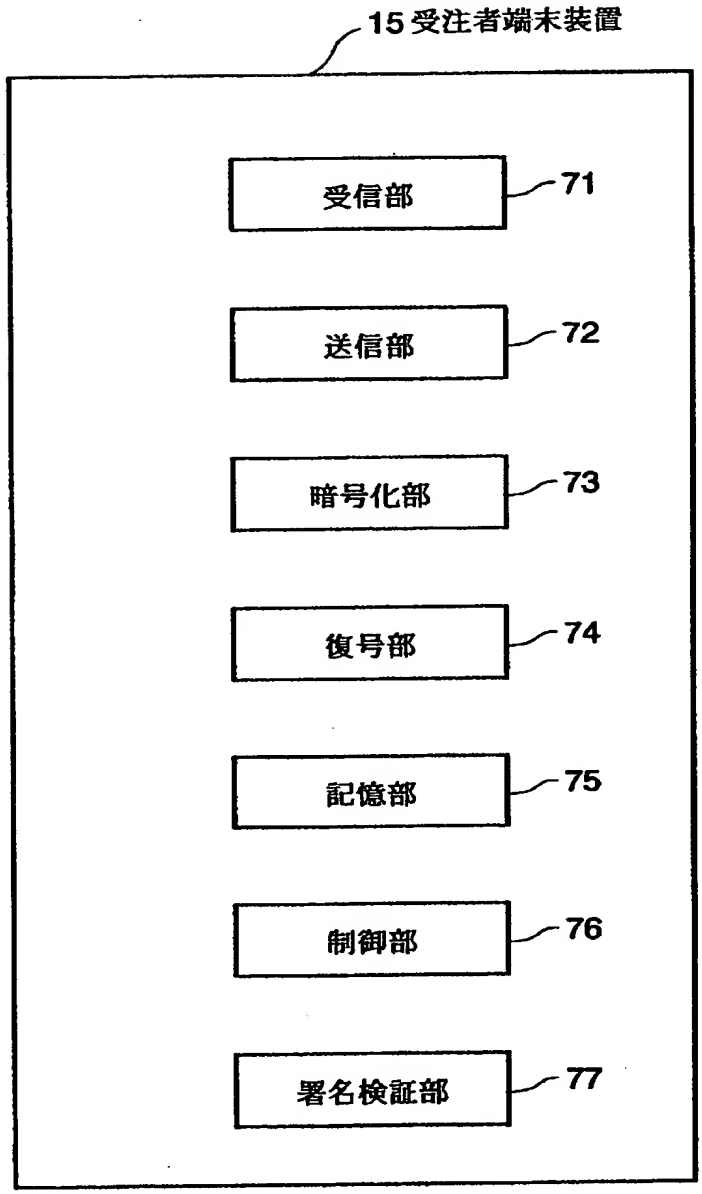
【図１】


1
ネットワーク銀行40
認証装置(A)
50
契約
契約
ネットワーク銀行41
認証装置(B)
51
受注者33
受注者端末装置
15
契約
商品配送
発注者31
発注者端末装置
11

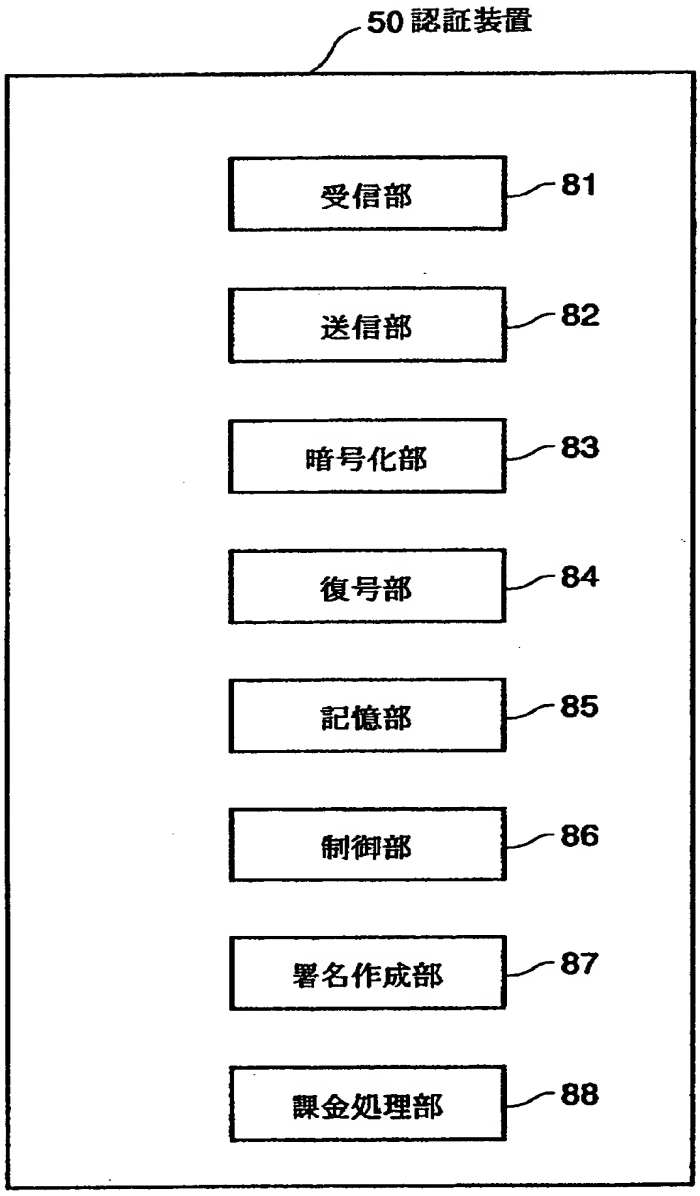
【図２】



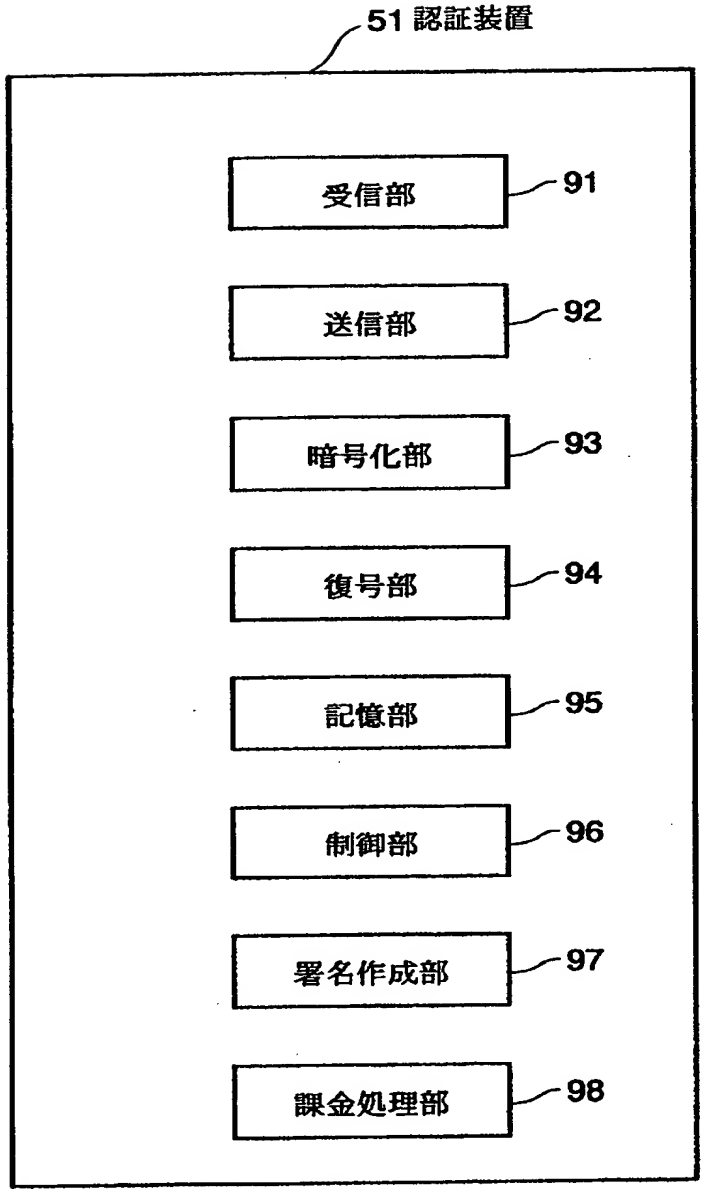
【図３】



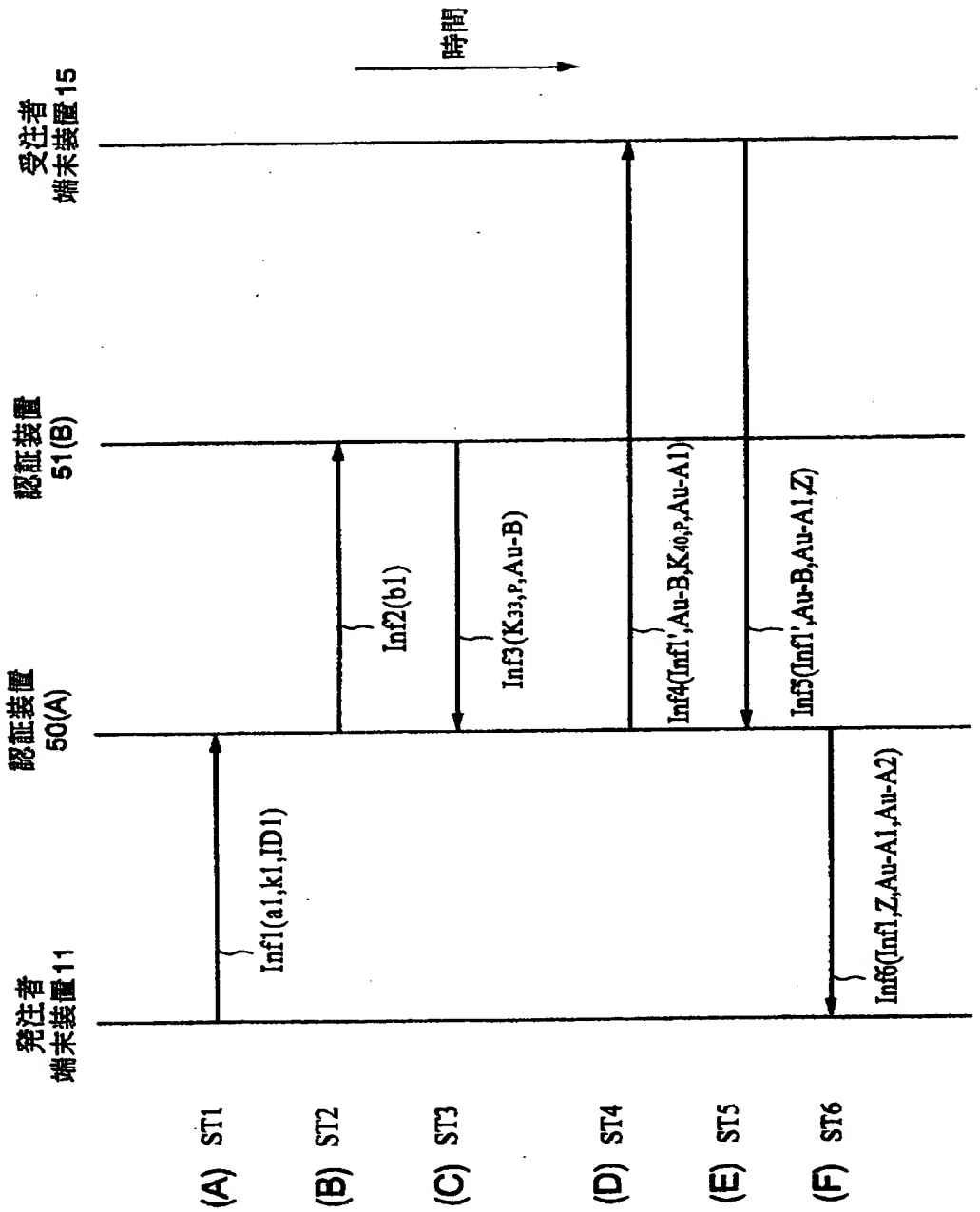
【図４】


50 認証装置
受信部
81
送信部
82
暗号化部
83
復号部
84
記憶部
85
制御部
86
署名作成部
87
課金処理部
88

【図５】


51 認証装置
受信部
91
送信部
92
暗号化部
93
復号部
94
記憶部
95
制御部
96
署名作成部
97
課金処理部
98

【図６】


時間
受注者端末装置15
認証装置51(B)
認証装置50(A)
発注者端末装置11
Inf1(a1,k1,ID1)
Inf2(b1)
Inf3(K33,P,Au-B)
Inf4(Inf1',Au-B,K40,P,Au-A1)
Inf5(Inf1',Au-B,Au-A1,Z)
Inf6(Inf1,Z,Au-A1,Au-A2)
(A) ST1
(B) ST2
(C) ST3
(D) ST4
(E) ST5
(F) ST6

【書類名】　　要約書

【要約】

【課題】　異なる認証機関と契約した利用者相互間の取り引きの認証を、利用者の個人情報を他の認証機関に提供することなく、高い信頼性で行うことができる認証装置を提供する。

【解決手段】　発注情報と受注者３３を特定する情報とを含む要求が発注者端末装置１１から認証装置５０に出されると、認証装置５０から５１に対して受注者３３を特定する情報が送信され、認証装置５０が５１から所定の署名情報を受信する。認証装置５０は、受注者端末装置１５に発注情報と上記署名情報とを送信し、受注者端末装置１５から個人キーを受信する。そして、認証装置５０は、当該取り引きの履歴を記憶すると共に発注者端末装置１１に所定の署名情報を送信する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社